CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
Valter Malkhasyan (SBN 348491)
vmalkhasyan@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

Counsel for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MAX ALPERSTEIN and ARYA SHOAEE, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

23ANDME, INC.,

Defendant.

Case No.: 5:23-cv-5541

CLASS ACTION COMPLAINT

1. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE SECTION 17200, *et seq*.
2. VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA") CAL. CIV. CODE SECTION 56, *et seq*.
3. VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA") CAL. CIV. CODE SECTION 1798, *et seq*.
4. VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, ("CLRA") CAL. CIV. CODE SECTION 1750, *et seq*.
5. NEGLIGENCE
6. INVASION OF PRIVACY
7. BREACH OF IMPLIED CONTRACT
8. CONVERSION
9. BREACH OF CONFIDENCE
10. UNJUST ENRICHMENT

DEMAND FOR JURY TRIAL

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Plaintiffs Max Alperstein and Arya Shoaee ("**Plaintiffs**"), individually and on behalf of all others similarly situated brings this action against Defendant 23andMe, Inc. ("**23andMe**" and/or "**Defendant**") and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Defendant is a San Francisco based company offering consumer-oriented genetic testing products and services to customers nationwide, where clients submit a saliva specimen to Defendant, which is then examined in a lab using genotyping. Through this testing, Defendant gathers significant amount of personal genetic information, accesses customers' entire ancestry, links customers to other individuals/relatives, discovers genetic predispositions to health issues, and gathers an enormous amount of health information for customers. This analysis produces insights about the individual's lineage and genetic tendencies linked to health concerns.

2. As part of its business model, Defendant harbors significant personally identifiable information ("**PII**") and protected health information ("**PHI**") for countless users of its services who trust that their sensitive and private information is safe. This information includes but is not limited to sensitive genetic information, names, sex, date of birth, genetic ancestry results, profile photos and geographical information. Unfortunately, this trust is misplaced and violated when Defendant knowingly subjects itself to the risk of cyberattacks.

3. Given the breadth and sensitivity of individuals' information at risk – the most private and critically important information such as genetic and medical information that cannot be changed, Defendant is an attractive target for a cyber-attack. Importantly, the genetic information not only affects the affected individuals, but also their relatives.

4. On or about October 6, 2023, Defendant issued a data breach notice on its website (the **"Data Breach"**) that customer profile information was compiled from individual 23andMe.com accounts without account users' authorization that contained both the **PII** and **PHI** of its customers (collectively, "**Private Information**").[1]

[1] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq*. ("**HIPAA**"), protected health information ("**PHI**") is considered to be individually identifiable

5. To date, Defendant has not yet disclosed full details of the Data Breach including when it occurred and the length of the exposure of Plaintiffs' and Class Members' Private Information or the results and findings of any investigation it undertook. Without such disclosure, questions remain as to the full extent of the cyberattack, the number of customers involved, the actual data compromised, and what measures, if any, Defendant has taken to secure the Private Information still in its possession. As a result, Plaintiffs and other Class Members are required to spend time and money in taking steps to protect themselves from the harmful effects of the Data Breach, while not knowing the full extent of the information exposed, or what other steps they could take to protect themselves.

6. Despite its awareness that it was storing highly sensitive Private Information that is often valuable and vulnerable to cyber attackers, Defendant failed to take the basic security precautions that could have protected Plaintiffs' and the Class's (defined below) sensitive data. For instance, Defendant could archive the data, preventing individuals from accessing any personal data by remote use of systems. Instead, Defendant used grossly inadequate computer systems and data security practices that allowed hackers to easily make off with the affected individuals' personal data. These extreme instances of data theft take time, and there were numerous steps along the way where any company following standard IT security practices would have foiled the hackers. But Defendant failed to take these basic precautions.

7. As far as is currently understood, the types of information that has been breached is of the type that federal and state law require companies to take security measures to protect. This includes, but is not limited to sensitive genetic information, names, sex, date of birth, genetic ancestry results, profile photos and geographical information.

---

information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. Summary of the HIPAA Privacy Rule, available at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Oct. 25, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

8. Defendant provided notice of the Data Breach to some but not all affected individuals. For instance, initially, Defendant refused to acknowledge that the data breach was occurring. Then, it finally notified some individuals, including Plaintiffs, downplaying the extent of the exposure.

9. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable security measures necessary to protect customers' Private Information. Defendant disregarded the rights of Plaintiffs and Class Members by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have reasonable or adequately robust computer systems and security practices to safeguard customers' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice regarding the Data Breach.

10. Upon information and belief, the mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information vulnerable to cyberattacks.

11. As a result of Defendant's failure to implement and follow reasonable security procedures, Plaintiffs' and Class Members' Private Information are now in possession of identity thieves. Plaintiffs and Class Members have suffered identity theft and fraud, diminished value in their sensitive information, have had to spend—and will continue to spend—significant amounts of time and money to protect themselves from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

12. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

13. Plaintiffs, on behalf of all others similarly situated, allege claims for (1) violation of the California Unfair Competition Law (Cal. Business & Professions Code § 17200, *et seq.*); (2) violation of the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq.*); (3) violation of California Consumers Privacy Act (Cal. Civ. Code § 17598.82 *et seq.*); (4) violation of California Consumers Legal Remedies Act, (Cal. Civ. Code Section 1750, *et seq.*); (5) negligence; (6) invasion of privacy; (7) breach of implied contract; (8) conversion; (9) breach of confidence; and (10) unjust enrichment.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages for identity theft, fraud, and time spent, reimbursement of out-of-pocket costs, adequate identity monitoring services funded by Defendant, and injunctive relief including improvements to Defendant's data security systems and practices to ensure they have reasonably sufficient security practices to safeguard customers' Private Information that remains in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future.

15. As a direct and proximate result of Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, Plaintiffs have incurred (and will continue to incur) economic damages, and other actual injury and harm, in the form of (i) actual identity theft or identity fraud; (ii) the untimely and/or inadequate notification of the Data Breach; (iii) unauthorized disclosure of their Private Information; (iv) breach of the statutorily-protected confidentiality of their Private Information; (v) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud caused by the Data Breach; (vi) the value of their time spent mitigating the impact of the Data Breach and mitigating increased risk of identity theft and/or identity fraud; (vii) deprivation of the value of their Private Information, for which there is a well-established national and international market;[2] and (vii) the impending, imminent, and ongoing increased risk of future

[2] Significantly, Defendant itself capitalizes on this inherent value of customers' Private Information by monetizing and selling this information to pharmaceutical entities for "research purposes."; Ben Marcus, *23andMe sold your genetic data to GSK: What this means for, your data, and your health*, CGLIFE, https://cglife.com/blog/23andme-sold-your-genetic-data-to-gsk-personalized-medicine-ethics/#:~:text=Earlier%20this%20summer%2C%20the%20often,signed%20up%20for%20the%20service (last accessed Oct. 26, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

identity theft, identity fraud, medical fraud, economic damages, and other actual injury and harm.

PARTIES

16. Plaintiff Max Alperstein, is and at all relevant times, was a California resident. Plaintiff Alperstein first started using Defendant's services approximately two to three years ago, in an effort to uncover more about his biological ancestry due to his adoption. With hopes of discovering more information about his biological roots, he meticulously completed a comprehensive family chart through Defendant's platform. Over the years, Plaintiff Alperstein has been diligent in updating the system with an array of sensitive information, including but not limited to specific medical conditions, submission of his DNA and other pertinent health details. As an active user, Defendant's services platform occasionally prompted Plaintiff Alperstein to additional health-related questions, to which he responded, further augmenting his profile with layers of intimate details.

17. As a direct result of Defendant's failure to safeguard this sensitive information, Plaintiff Alperstein received a notification that his DNA Relatives profile was among those compromised in the recent Data Breach. The breach divulged numerous sensitive aspects of his profile including but not limited to his chosen relationship labels (whether masculine, feminine, or neutral), the predicted relationships and the exact percentage of DNA shared with his matches, comprehensive ancestry reports, and corresponding DNA segments, his geographical location, the birthplaces of ancestors, associated family names, his birth year, and even a direct link to his diligently constructed Family Tree. To his knowledge, Plaintiff Alperstein has not had his genetic information compromised through any other data breaches. Plaintiff Alperstein would not have trusted Defendant with his Private Information had he known such sensitive information was vulnerable to cyberattacks.

18. Plaintiff Arya Shoaee, is and at all relevant times, was a resident of California. Plaintiff Shoaee began using Defendant's services in March of 2021, driven by a curiosity to trace back his ancestral lineage. To discover a detailed map of his familial heritage, Plaintiff Shoaee entered comprehensive data into Defendant's platform about his parents, relatives, their respective birthdays, and places of birth. In addition to this, Plaintiff Shoaee also input personal identifying

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

information about himself. Throughout his association with the Defendant's platform, Plaintiff Shoaee consistently provided these details, ensuring his profile was as detailed and thorough as possible, capturing the intricate nuances of his family's history.

19. As a direct result of Defendant's failure to safeguard this sensitive information, sensitive aspects of Plaintiff Shoaee's profile were compromised—including but not limited to his chosen relationship labels (whether masculine, feminine, or neutral), the predicted relationships and the exact percentage of DNA shared with his matches, comprehensive ancestry reports, and corresponding DNA segments, his geographical location, the birthplaces of ancestors, associated family names, his birth year, and even a direct link to his diligently constructed Family Tree. To his knowledge, Plaintiff Shoaee has not had his genetic information compromised through any other data breaches. Plaintiff Shoaee would not have trusted Defendant with his Private Information had he known such sensitive information was vulnerable to cyberattacks.

20. Defendant 23andMe Genetics Corporation is a Delaware corporation with its principal place of business in San Francisco, California.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

22. This Court has personal jurisdiction over Defendant because Defendant is headquartered in California, its principal place of business is in California, and it regularly conducts business in California.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District, and Defendant is in this District, and has caused harm to Plaintiffs and Class Members residing in this District.

24. Defendant is subject to personal jurisdiction in California based upon sufficient minimum contacts which exist between Defendant and California. Defendant is incorporated in

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

California, maintains its principal place of business in California, is authorized to conduct and is conducting business in California.

FACTUAL ALLEGATIONS

Data Breaches and the Market for PII/PHI

25. Data breaches in the United States have become commonplace – from nearly 125 million breaches in just the fourth quarter of 2020, to approximately 15 million breaches in the third quarter of 2022 (increasing 167% compared to the previous quarter) – with the goal of criminals being to monetize the stolen data.[3]

26. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data—including but not limited to identity theft, fraud, decline in credit, inability to access healthcare, as well as legal consequences.[4]

27. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems could take more than a year.[5]

28. The U.S. Government Accountability Office has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.[6] In the same report, the Government Accountability Office noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[7]

[3] Ani Petrosyan, *Number of Data Records Exposed Worldwide From 1st Quarter 2020 to 3rd Quarter 2022*, STATISTA, https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ (last accessed on Oct. 26, 2023).
[4] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/wp-content/uploads/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last accessed on Oct. 15, 2023).
[5] Erika Harrell, *Victims of Identity Theft, 2014,* U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed on Oct. 15, 2023).
[6] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft Services* (March 2019), https://www.gao.gov/assets/700/697985.pdf (last accessed on Oct. 15, 2023).
[7] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

29. When companies entrusted with people's data fail to implement industry best practices, cyberattacks and other data exploitations can go undetected for a long period of time. This worsens the ramifications and can even render the damages irreparable.

30. PII is a valuable commodity for which a black market exists on the dark web, among other places. Personal data can be worth from $1,000 - $1,200 on the dark web[8, 9] and the legitimate data brokerage industry is valued at more than $250 billion dollars. The value is even higher for the PII that cannot be changed, including medical information and genetic information at issue here.

31. In this black market, criminals seek to sell the spoils of their cyberattacks to identity thieves who desire the data to extort and harass victims, take over victims' identities in order to open financial accounts, and otherwise engage in illegal financial transactions under the victims' names.

32. PII and PHI have a distinct, high value—which is why legitimate companies and criminals seek to obtain and sell it. As alleged in more detail below, there is a growing market for individuals' data.[10]

33. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems could take more than a year. Medical information in particular is extremely valuable to identity thieves, and thus, the medical industry has also experienced disproportionally higher numbers of data theft events than other industries. According to a report by the Health Insurance Portability and Accountability Act ("**HIPAA**") Journal, "healthcare data breach statistics clearly show there has been an upward trend in data

[8] Ryan Smith, *Revealed-how much is personal data worth on the dark web*?, INSURANCE BUSINESS MAGAZINE (May 1, 2023), https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx (last accessed Oct. 26, 2023).

[9] Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*, MARKETWATCH (June 6, 2018), https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20 (last accessed Oct. 26, 2023).

[10] Emily Wilson, *The Worrying Trend of Children's Data Being Sold on the Dark Web*, TNW (Feb. 23, 2019), https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/ (last accessed Oct. 15, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

breaches over the past nine (9) years, with 2018 seeing more data breaches reported than any other year since records first started being published."[11]

34. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[12] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

35. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Defendant knew or, at the very least, should have known that the Private Information at issue (PII/PHI) — is highly valuable to criminals.

36. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. Yet, what is even more alarming about the data breach in question is its depth of the data involved and compromised as the direct result from Defendant's failure to ensure compliance with the data breach practices. The Data Breach surpasses mere medical identity theft; it compromised the specific and unique individuals' genetic identity, encompassing data that affects **both the individual and their family members.** Unlike other forms of data, this genetic information is immutable and cannot be altered, thus, its exposure and misuse impact multiple individuals and, in many cases, entire families, due to the interconnected nature of genetic data.

37. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[13]

---

[11] *Healthcare Data Breach Statistics*, THE HIPPA JOURNAL, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last accessed Oct. 26, 2023).
[12] *What To Know About Identity Theft*, FEDERAL TRADE COMMISSION, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Oct. 25, 2023).
[13] *The Rise Of Medical Identity Theft In Healthcare*, KFF HEALTH NEWS, https://kffhealthnews.org/news/rise-of-indentity-theft/ (last accessed Oct. 26, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

38. Similarly, the FBI Cyber Division, in an April 8, 2014, Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[14]

39. A study done by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[15] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

40. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

41. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[16] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[17]

42. Importantly, Defendant itself recognizes the inherent monetary value of consumers' Private Information. In its own business practice, Defendant monetizes consumers' sensitive Private information, selling parts of it to pharmaceutical companies and utilizing portions of this data for

---

[14] *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION, https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last accessed Oct. 26, 2023).

[15] Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last accessed on Oct. 26, 2023).

[16] *Medical ID Theft Checklist*, https://www.identityforce.com/blog/medical- id-theft-checklist-2 (last accessed Oct. 25, 2023).

[17] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft- healthcare.pdf (last accessed Oct. 25, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

other market-oriented purposes, including research that is ultimately channeled for commercial purposes.[18]

Defendant's Business Model

43. Defendant 23andMe was founded in 2006, when it started offering unique direct-to-consumer genetic testing services.[19] Defendant is based in California, from where it markets and advertises its products and services consisting of variety of tests each of which gathers PII/PHI. Through Defendant's products and services, consumers submit their saliva samples to be examined in a laboratory setting using SNP genotyping (the laboratory which is located in California), which then provides insights regarding consumers' genetic lineage and potential health-related predispositions.[20] The findings are then made accessible online. Therefore, each individual's genetic information and other medical information is analyzed and compiled in a laboratory in California.

44. Defendant supplies consumers with DNA testing kits that reveal insights about health, individual genetic attributes, and ancestral lineage.[21] Once the saliva sample is taken, customers attach the barcode to the collection tube and send it back to Defendant. The company offers a comprehensive health and ancestry products and services, sharing reports on genetic health risks, carrier statuses, wellness, and pharmacogenetics. Additionally, an annual membership is available, encompassing all the aforementioned services plus continuous genetic updates. The pricing for these services and memberships vary.

45. However, each of the products and services would be entirely worthless or at least valued significantly less, had Defendant accurately represented these products/services –

[18] Ben Marcus, *23andMe sold your genetic data to GSK: What this means for, your data, and your health*, CGLIFE, https://cglife.com/blog/23andme-sold-your-genetic-data-to-gsk-personalized-medicine-ethics/#:~:text=Earlier%20this%20summer%2C%20the%20often,signed%20up%20for%20the%20service (last accessed Oct. 26, 2023).

[19] Cynthia McFadden, *DNA test company 23andMe now fueling medical research*, NBC NEWS (Jan. 17, 2019), https://www.nbcnews.com/health/health-news/dna-test-company-23andme-now-fueling-medical-research-n958651 (last accessed Oct. 26, 2023).

[20] *How 23andMe Reports Genotype*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/212883677-How-23andMe-Reports-Genotypes (last accessed Oct. 25, 2023).

[21] 23&ME, https://www.23andme.com (last accessed Oct. 25, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

specifically that Defendant's compiling of this information and offering of services was conducted with the mediocre security measures and inadequate privacy protocols.

46. Given the intricacies of its services, Defendant necessarily retains customers' Private Information digitally in its system. Globally, the company boasts over 14 million customers and has, by December 2022, conducted genotyping for over 5 million individuals.[22]

47. As a condition of engaging in its Products and services, Defendant requires that these customers entrust them with highly confidential Private Information.

48. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

49. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, and, as current and former customers, they relied upon Defendant to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

50. The safeguarding of users' Private Information is paramount for customers. Consequently, Defendant has the responsibility to ensure this sensitive data is adequately protected from unauthorized entities.

The Data Breach at Issue

51. On October 6, 2023, Defendant announced in a Blog on its website that customers' accounts had been accessed by unauthorized individuals. The announcement titled "Addressing Data Security Concerns" read:

> "We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.

[22] Joseph Menn, *Genetic tester 23andMe's hacked data on Jewish users offered for sale online*, THE WASHINGTON POST (Oct. 6, 2023), https://www.washingtonpost.com/technology/2023/10/06/23andme-hacked-data/ (last accessed Oct. 25, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

> "We believe that the threat actor may have then, in violation of our Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service."[23]

52. Defendant's Blog notification fails to disclose how many individuals were affected, what information was accessed other than "customer profile information" and "information about users' DNA Relatives profiles"[24] and when and for how long the information was accessed.

53. Defendant's Blog notification failed to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed its customer/employee's e-mail accounts, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach was a system-wide breach, whether servers storing information were accessed, and how many customers were affected by the Data Breach.

54. Even worse, Defendant has not offered any identity monitoring to all affected individuals.

55. Indeed, October 7, 2023, NBC News reported and confirmed the following: *A database that has been shared on dark web forums and viewed by NBC News has a list of 999,999 people who allegedly have used the service. It includes their first and last name, sex, and 23andMe's evaluation of where their ancestors came from. The database is titled "ashkenazi DNA Data of Celebrities," though most of the people on it aren't famous, and it appears to have been sorted to only include people with Ashkenazi heritage.*[25]

56. In addition, NBC News further reported that "A user on a popular hacker forum had claimed to have made a larger database of users for sale earlier this week."[26]

57. Three days later, on October 9, 2023, Defendant updated its October 6, 2023, announcement and failed to disclose any useful additional information other that its investigation

[23] *Addressing Data Security Concerns*, 23ANDME, https://blog.23andme.com/articles/addressing-data-security-concerns (last accessed Oct. 25, 2023).
[24] *Id.*
[25] Kevin Collier, *23andMe user data targeting Ashkenazi Jews leaked online*, NBC NEWS (Oct. 7, 2023) https://www.nbcnews.com/news/us-news/23andme-user-data-targeting-ashkenazi-jews-leaked-online-rcna119324# (last accessed Oct. 25, 2023).
[26] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

continues, and it "engaged the assistance of third-party forensic experts" and is working with "federal law enforcement officials."[27]

Defendant's Duty to Safeguard User's Private Information

58. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including HIPAA and the Federal Trade Commission Act ("**FTCA**"), 15 U.S.C. § 45.

59. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[28]

60. Based on information and belief, Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Defendant's security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security

[27] *Addressing Data Security Concerns*, 23&ANDME, https://blog.23andme.com/articles/addressing-data-security-concerns (last accessed Oct. 25, 2023).
[28] *What is Considered Protected Health Information Under HIPAA?,* HIPAA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last accessed Oct. 26, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, et seq.;

i. Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

61. In addition to HIPPA obligations, Defendant was also prohibited by the Federal Trade Commission Act ("**FTC Act**") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("**FTC**") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

62. The Federal Trade Commission ("**FTC**") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices.

63. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[29] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

[29] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Oct. 25, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

understand their network's vulnerabilities; and implement policies to correct any security problems.

64. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("**FTCA**"), 15 U.S.C. § 45.

66. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

67. The FTC recommends that businesses have a comprehensive communication plan that reaches all affected audiences—employees, customers, investors, business partners, and other stakeholders—in the case of a data breach. This plan should be designed to quickly notify people that their personal information has been compromised so that they can take steps to reduce the chance that their information will be misused.

68. The FTC also instructs businesses to provide detailed notices to affected parties that "clearly describe what you know about the compromise." This information, at a minimum, should include: "how it happened; what information was taken; how the thieves have used the information (if you know); what actions you have taken to remedy the situation; what actions you are taking to protect individuals, such as offering free credit monitoring services; and how to reach the relevant contacts in your organization."[30]

///

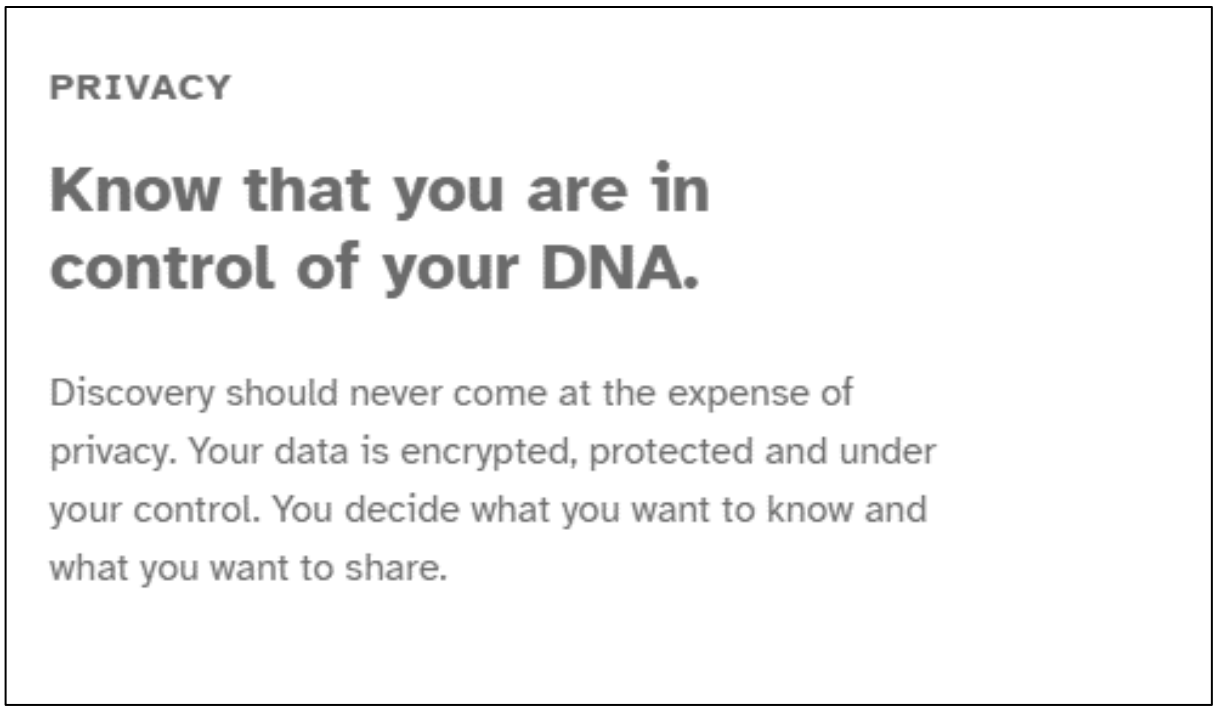
///

[30] *Data Breach Response: A Guide for Business*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed Oct. 26, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Defendant's Promises of Data Security and Privacy

69. Beyond Defendant's legal obligations to protect the confidentiality of patients' Private Information, Defendant makes numerous promises to its customers that it will maintain the security and privacy of their Private Information. On its website, where Defendant sells its own products and services, Defendant prominently (including on its main page) makes a variety of false misrepresentations regarding its privacy and protections:[31]



70. Defendant also provides an option to "Learn More" under the falsely promised protections listed above, which directs consumers to the Privacy page, on which Defendant extensively continues to misrepresent that consumers' Private Information will be protected:[32]

///

///

///

///

///

[31] 23ANDME, https://www.23andme.com (last accessed Oct, 26, 2023).
[32] *Privacy,* 23ANDME, https://www.23andme.com/privacy/ (last accessed Oct. 25, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

a. "Your data is fiercely protected by security practices that are regularly reviewed and updated."[33]

b. "Your genetic information deserves the highest level of security, because without security, you can't have privacy."[34]

c. "We exceed industry data protection standards and have achieved 3 different ISO certifications to demonstrate the strength of our security program."[35]

d. "We encrypt all sensitive information and conduct regular assessments to identity security vulnerabilities and threats."[36]

71. Defendant makes its prominent misrepresentations about privacy protections on the pages where it sells its products and services, to ensure that consumers purchasing products and services rely on these statements and are enticed to purchase the products and services.

72. Consumers who purchased Defendant's products and services, reasonably relied on these false and misleading representations regarding data protection and security, prior to making decisions to purchase Defendant's products and services. In fact, data protection and security is **the**

[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

most important factor, which affects their purchasing decisions for Defendant's products and services. If consumers knew that their information would not be kept private/be protected or that Defendant does not implement adequate security measures to prevent disclosures of their information, they would not purchase the products and services.

73. In fact, Defendant knows that this is one of the most important purchasing factors in selecting their products and services. For these reasons, Defendant dedicates several extensive sections of its website to prominently over-promise and misrepresent its security measures, stating that "You are free to explore your DNA with confidence . . . rest assured knowing that . . . we will not share your genetic data . . . exceed industry data protection standards . . . encrypt all sensitive information . . ." (among other things).

74. Furthermore, in its Privacy Statement, under Security Measures, Defendant explicitly notes that:

a. "Our team regularly reviews and improves our security practices to help ensure the integrity of our systems and your Personal Information."[37]

b. "We believe everyone deserves a safe place to discover and understand their DNA, which means we need to keep our platform a safe place for all. We use information to monitor, detect, prevent, investigate and mitigate any suspected or actual fraud, prohibited or illegal behaviors on our Services, to combat spam, and other behaviors or actions that break the promises we outline in our Terms of Service."[38]

75. In further emphasizing their commitment to customer privacy, Defendant hosts a video on its website detailing the measures it takes to safeguard customers' data.

///

///

///

///

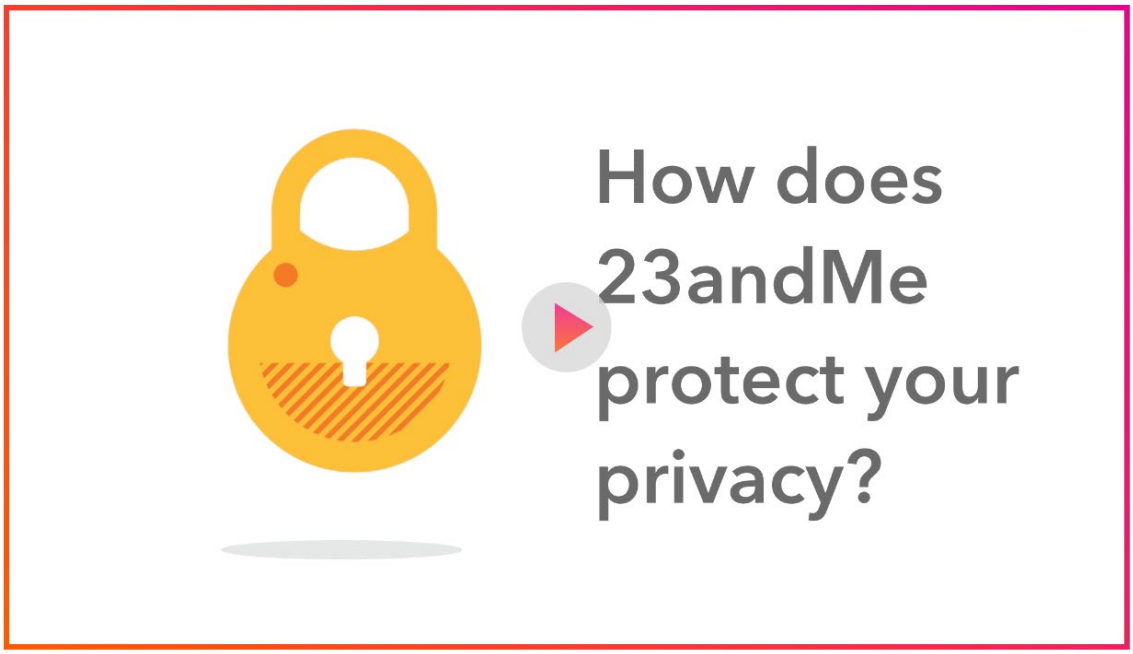
///

///

[37] *Privacy Statement,* 23ANDME, https://www.23andme.com/legal/privacy/full-version/ (last accessed Oct. 25, 2023).

[38] *How We Use Your Information*, 23ANDME, https://www.23andme.com/legal/how-we-use-info/ (last accessed Oct. 25, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com



76. Within this video, Defendant outlines "key ways" by which consumers' both DNA and Private Information are protected. Notably, among those "key ways" is Defendant's supposed integration of *"strong security"* and privacy practices at every phase of the data handling and analysis process.[39]

77. Defendant goes on to describe how customers' Private Information may be used and disclosed for each category of uses or disclosures, none of which provide it a right to expose customers' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

78. By failing to protect Plaintiffs' and Class Members' Private Information, and by allowing the Data Breach to occur, Defendant broke these promises to Plaintiffs and Class Members.

Defendant's Failure to Live Up To Its Promises to Ensure Robust Data Privacy and Security Protections

79. Defendant also repeatedly represented and promised consumers that it is committed to the robust data privacy and security protections, enabled by the General Data Protection Regulations ("**GDPR**") compliance.[40] These promises suggest to consumers that Defendant has

[39] *Privacy*, 23ANDME, https://www.23andme.com/privacy/ (last accessed Oct. 26, 2023).
[40] *Data Protection*, 23ANDME, https://www.23andme.com/gdpr/ (last accessed Oct. 26, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

implemented robust privacy practices and security protections as a result.

80. Under the GDPR requirements, companies are also required to hire a data protection officer in charge of conducting regular assessments and audits to ensure compliance, maintaining records of all data processing activities conducted by the company, training organization employees to ensure compliance, building greater data protection awareness for the employees, vendors and individuals involved, and prioritizing the enhancement of data processes.

81. Despite Defendant's representations of its compliance, Defendant failed to:

a. ensure that it created robust policies and security protections, and yet failed to do so.

b. train and/or monitor its employees, vendors, and agents who had access to the Private Information.

c. develop robust internal policies, processes, and security protocols to prevent the data breach.

d. develop robust internal policies, processes, and security protocols to timely detect the data breach;

e. develop robust internal policies, processes, and security protocols to timely respond to the data breach;

f. develop robust internal policies, processes, and security protocols to alert of the data breach affected individuals.

g. conduct regular audits to prevent the data breach and assure awareness of and compliance with the security protocols.

h. design the appropriate procedures to prevent the data breach; and deploy the industry standards and security protocols to prevent the data breach.

i. create internal security protocols and policies for the team members, and build awareness about the data protections.

82. The descriptions of Defendant's negligence and failures to implement sufficient and adequate protection measures listed above are not exhaustive, and the full extent of Defendant's failures to implement adequate protection measures remains unknown.

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

83. Furthermore, under the GDPR regulations, Defendant was obligated to provide notice of the data breach no later than 72 hours, and yet, it failed to do so. To date, the complete notice has not been given, nor complete disclosures were provided.

Defendant's Failure to Implement Adequate Security Measures

84. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendant on notice, long before the Data Breach, that (1) cybercriminals were targeting large, public companies such as Defendant; (2) cybercriminals were ferociously aggressive in their pursuit of large collections of Private Information like that in possession of Defendant; (3) cybercriminals were selling large volumes of PII/PHI and corporate information on Dark Web portals; and (4) the threats were increasing.

85. Had Defendant been diligent and responsible, it would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key avoidable causes for data security incidents are:

- Lack of a complete risk assessment, including internal, third-party, and cloud-based systems and services;
- Not promptly patching known/public vulnerabilities, and not having a wayto process vulnerability reports;
- Misconfigured devices/servers;
- Unencrypted data and/or poor encryption key management and safeguarding;
- Use of end-of-life (and thereby unsupported) devices, operating systems,and applications;
- Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;
- Failure to block malicious email; and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

- Users succumbing to business email compromise (BEC) and social exploits.[41]

86. Data security experts advise that "the vast majority of data breaches are preventable" if companies follow widely-available advice on data security practices, including "continually audit[ing] and reevaluat[ing]" their data security practices; being aware of and working proactively to counter cybercriminals' evolving techniques and approaches; and training and re-training their employees.[42]

87. Defendant represents itself as the leading entity which "exceed industry data protection standards"[43] and yet, it failed to adhere to the well-known causes for the data breaches and implement protocols to prevent said data breach.

The Sensitivity of Patients' Health Data Demands Heightened, Vigilant, Protection.

88. As a provider of DNA and genetic testing services, Defendant knew, or should have known, the importance of safeguarding its customers' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's customers as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

89. The ramifications of Defendant's failure to keep customers' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

90. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

---

[41] Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), https://www.proofpoint.com/us/security-awareness/post/ota-report-indicates-93-security-breaches-are-preventable (last accessed Oct. 25, 2023).

[42] Nate Nead, *How To Prevent A Data Breach In Your Company*, FORBES BUSINESS COUNSEL, FORBES (Jul. 30, 2021), https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=3828f7b918da (last accessed Oct. 25, 2023).

[43] *Privacy,* 23ANDME, https://www.23andme.com/privacy/ (last accessed Oct. 26, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

91. Defendant further owed and breached its duty to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems. In other words, even if a company negligently left the "bank vault" open (as Defendant did), it would still have videos monitoring the bank vault, and alarms that would go off if intruders tried to leave with the loot. Defendant failed to implement standard monitoring and alerting systems.

92. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause misuse to Plaintiffs' and Class Members' Private Information as detailed above. Plaintiffs and Class Members are now at a heightened and increased risk of identity theft and medical fraud.

93. Identity theft poses significant risks. While some impacted individuals can address their issues promptly, others are forced to expend significant time and money to rectify the damage done to their reputation and credit history. Often, this leads to missed employment prospects, rejections for loans related to education, housing, or vehicles due to tainted credit histories. In extreme cases, impacted individuals could even face false criminal charges.

94. Indeed, the U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."

95. Additional risks include medical fraud, unauthorized loans taken in the victim's name, new utility accounts under their name, fraudulent tax returns, and illicit credit card activities.

96. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

or integrity of such sensitive information.

97. Despite possessing the means to prevent the Data Breach,[44] Defendant neglected to adequately implement and enforce data security precautions. Defendant had an obligation to protect sensitive customer data.

98. Had Defendant addressed the shortcomings in its security infrastructure and heeded expert-recommended safety protocols, the breaches and subsequent theft of Private Information belonging to the Plaintiffs and Class Members could have been avoided.

99. Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in their agreements with Defendant. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value of the genetic testing services with data security protection they paid for and the services they received.

100. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure, and vulnerable to attack, Defendant would have been unable to continue in business, and would have been forced to adopt reasonable data security measures and comply with the law. Plaintiffs and millions of other consumers would not have entrusted Defendant with their sensitive data.

101. Defendant's failure to protect and safeguard such sensitive information is due to a series of systemic failures. These include an incomplete risk assessment of both internal and external systems, delays in patching known vulnerabilities, misconfigurations of servers and devices, inadequate data encryption and key management, reliance on outdated and unsupported technologies, employee errors leading to unintentional disclosures, an inability to fend off malicious emails, and vulnerabilities to email compromises and social exploits. This pattern of neglect and oversight by the Defendant resulted in the Data Breach.

///

[44] Defendant's *2023 Third Quarter Financial Results* show revenue of $290-300 million. See https://investors.23andme.com/news-releases/news-release-details/23andme-reports-fy2023-third-quarter-financial-results#:~:text=23andMe%20is%20raising%20its%20full,of%20%24325%20to%20%24335%20million.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Summary of Actual Economic and Noneconomic Damages

102. In sum, Plaintiffs and similarly situated individuals were injured as follows:

a. Theft of their Private Information and the resulting loss of privacy rights in that information;

b. Improper disclosure of their Private Information;

c. Loss of value of their Private Information;

d. The amount of ongoing reasonable identity defense services made necessary as mitigation measures;

e. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs and Class Members are now exposed to;

f. Ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach;

g. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach;

h. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this Data Breach;

i. The continued risk of their Private Information, which remains in the possession of Defendant, being is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession.

103. In addition to the harms described above, the Private Information stolen can be combined with personal information from other sources such as publicly available information, social media, etc. to create digital dossiers of people to commit further identity theft or medical fraud.

104. Defendant has not offered or provided victims any identity monitoring services or fraud protection to impacted individuals. In fact, Defendant does not appear to be taking any measures to assist Plaintiffs and Class Members other than advising them to strengthen their password and activate multi-factor authentication on their accounts.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

105. As a direct and proximate result of Defendant's Data Breach, and its failure to protect the Private Information, Plaintiffs and Class Members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, social engineering, and other misuses of their Private Information, as well as an increased risk to their personal safety; ongoing monetary loss and economic harm, including loss of value of their PII/PHI; loss of value of privacy and confidentiality of the stollen Private Information – especially given that this information cannot be changed; illegal sales of compromised Private Information; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost time; and other injuries. Plaintiffs and the Class Members have continued interest in ensuring that their personal information is and remains safe and should be entitled to injunctive and equitable relief.

CALIFORNIA LAW SHOULD BE APPLIED TO THE NATIONWIDE CLASS

106. The State of California has a significant interest in regulating the conduct of businesses operating within its borders. California seeks to protect the rights and interests of all California residents and citizens of the United States against a company headquartered and doing business in California. California has a greater interest in the nationwide claims of Plaintiffs and members of the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

107. The corporate headquarters of Defendant are in San Francisco, California, which is the "nerve center" of its business activities – the place where its officers direct, control, and coordinate the company's activities, including its data security functions and policy, financial, and legal decisions. Further, upon information and belief, all managerial decisions stem from California, the representations on Defendant's website originate from California, and Defendant's response to the Data Breach, and corporate decisions surrounding such response, was made from California. Therefore, application of California law to the Class is appropriate.

108. Defendant's privacy officers and administrators in charge and/or responsible for making decisions concerning data protections are located in San Francisco, California. Defendant's negligence, and failures to implement the necessary procedures, stem from California.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

109. Furthermore, the data lab where Plaintiffs' and other Class Members' data is collected and kept by the Defendant is also in California. Upon information and belief, even Defendant's data centers are located in California, San Francisco area.

110. Defendant's important decisions concerning data and privacy emanate from California.

111. Therefore, California has significant contacts and significant aggregation of contacts to the claims of each class member – because this is where the data was gathered, PII/PHH was collected through testing, and where decisions regarding mishandling of data occurred, affecting all class members.

112. Application of California law to the Class is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Class.

113. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the nationwide common law claims of all members of the Class. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, California's Unfair Competition Law and Confidentiality of Medical Information Act may be applied to non-resident plaintiffs against Defendant.

114. Furthermore, given Defendant's extensive connections with California, Defendant's headquarters in San Francisco, deceptive practices emanating from California, Defendant's requirement that each Class Members send their samples to California, and injuries occurring in California (where Defendant mishandled data) – California law should apply to the nationwide class.

CLASS ALLEGATIONS

115. Plaintiffs bring this action on their own behalf and on behalf of all other persons similarly situated. The Class which Plaintiffs seek to represent comprises:

> **Nationwide Class**: All persons in the United States whose Private Information was accessed, compromised, or stolen in the data breach first announced by Defendant on or about October 6, 2023.
>
> **California Subclass:** All persons in the state of California whose

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Private Information was accessed, compromised, or stolen in the data breach first announced by Defendant on or about October 6, 2023. (collectively, the **"Class"**).

116. The Class is comprised of numerous of individuals throughout the United States and the state of California. The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties.

117. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the Class was exposed to the same common and uniform false and misleading advertising and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class Members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

b. Whether Defendant's conduct is an unfair business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

c. Whether Defendant's failure to implement effective security measures to protect Plaintiffs' and the Class's Private Information was negligent;

d. Whether Defendant represented to Plaintiffs and the Class that it would protect Plaintiffs' and the Class Members' Private Information;

e. Whether Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

f. Whether Defendant breached a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

g. Whether Class Members' Private Information was accessed, compromised, or stolen in the breach;

h. Whether Defendant's conduct caused or resulted in damages to Plaintiffs and the Class;

i. Whether Defendant failed to notify the public of the breach in a timely and adequate manner;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

j. Whether Defendant knew or should have known that its systems were vulnerable to a data breach;

k. Whether Defendant adequately addressed the vulnerabilities that allowed for the data breach; and

l. Whether, as a result of Defendant's conduct, Plaintiffs and the Class are entitled to injunctive relief.

118. Plaintiffs' claims are typical of the claims of the proposed Class, as Plaintiffs and the members of the Class were harmed by Defendant's uniform unlawful conduct.

119. Plaintiffs will fairly and adequately represent and protect the interests of the proposed Class. Plaintiffs have retained competent and experienced counsel in class action and other complex litigation.

120. Plaintiffs and the Class have suffered injury in fact as a result of Defendant's false, deceptive, and misleading representations.

121. Plaintiffs would not have entrusted Defendant with their Private Information but for the reasonable belief that Defendant would safeguard their Private Information.

122. The Class is identifiable and readily ascertainable. Notice can be provided using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

123. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually.

124. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by Defendant's conduct would increase delay and expense to all parties. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision.

125. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Class as a whole. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual members of the Class that would establish incompatible standards of conduct for Defendant.

126. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class Members' claims, few, if any, Class Members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, the Class Members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law.

127. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, identity monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

///

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

COUNT ONE

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW

BUSINESS & PROFESSIONS CODE SECTION 17200 *et seq.*

(On behalf of Plaintiffs and the Nationwide Class)

128. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

A. "Unfair" Prong

129. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to individuals and the injury is one that the individuals themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal.App.4th 1394, 1403 (2006).

130. Defendant's conduct of failing to protect and secure its data-holding systems as alleged herein does not confer any benefit to individuals.

131. Defendant's conduct as alleged herein causes injuries to individuals who do not receive security consistent with their reasonable expectations.

132. Defendant's conduct as alleged herein causes injuries to individuals who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

133. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively declared public policy that seeks to protect individuals' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56.

134. Individuals cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

135. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

136. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

137. Defendant could have furthered its legitimate business interests in ways other than by unfair conduct.

138. Defendant's conduct threatens individuals by misleadingly advertising its systems as "secure" and exposing individuals' Private Information to hackers. Defendant's conduct also threatens other entities, large and small, who play by the rules.

139. All of the conduct alleged herein occurs and continues to occur in Defendant's enterprise. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

140. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

141. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs relied on and trusted that Defendant would keep their PII/PHI safe and secure in part based on Defendant's representations regarding its security measures. Plaintiffs accordingly provided their PII/PHI to Defendant reasonably believing and expecting that this information would be safe and secure. Plaintiffs and the Class would not have given Defendant sensitive Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect individuals' Private Information. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant's unfair and unlawful practices.

B. "Unlawful" Prong

142. California Business and Professions Code Section 17200, et seq., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

143. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq*.

144. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

145. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56 (requiring reasonable data security measures) and California common law. Defendant failed to timely notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with California common law.

146. Defendant knew or should have known of its unlawful conduct.

147. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

148. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

149. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

150. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

151. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs and the Class would not have trusted Defendant with their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect individuals' Private Information. Additionally, Plaintiffs and members of the Class seek and request an order awarding Plaintiffs and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

the Class restitution of the money wrongfully acquired by Defendant's unfair and unlawful practices.

COUNT TWO

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT

CAL. CIV. CODE Section 56, *et seq*.

(On behalf of Plaintiffs and the Nationwide Class)

152. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

153. Defendant is subject to the requirements and mandates of California Confidentiality of Medical Information Act, Cal. Civ. Code § 56 *et seq*. ("CMIA") because Defendant had the "purpose of maintaining medical information to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual."

154. Section 56.36 allows an individual to bring an action against a "person or entity who has negligently released confidential information or records concerning him or her in violation of this part."

155. Plaintiffs and Class Members are customers of Defendant, as defined in Civil Code § 56.05(k).

156. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care ... regarding a patient's medical history, mental or physical condition, or treatment."

157. The CMIA defines individually identifiable information as "medical information [that] includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patients name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." Cal. Civ. Code § 56.050.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

158. As is currently understood, the compromised data at issue includes but is not limited to sensitive genetic information, names, sex, date of birth, genetic ancestry results, profile photos and geographical information.

159. As a result of the Data Breach, Defendant has misused, disclosed, and/or allowed third parties to access and view Plaintiffs' and Class Members' PHI without their written authorization compliant with the provisions of Civil Code §§ 56, *et seq*.

160. Defendant lawfully came into possession of the Plaintiffs' and Class Members' medical information and had a duty pursuant to Section 56.06 and 56.101 of the CMIA to maintain, store and dispose of the Plaintiffs' and Class Member's medical records in a manner that preserved its confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, store, abandonment, destruction, or disposal of confidential medical information.

161. Defendant further violated the CMIA by failing to use reasonable care, and in fact, negligently maintained the Plaintiffs' and Class Members' medical information.

162. As a direct and proximate result of Defendant's violations of the CMIA, Plaintiffs and the Class Members have been injured and are entitled to compensatory damages, punitive damages, and nominal damages of one-thousand dollars ($1,000) for each of Defendant's violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

COUNT THREE

VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

CALIFORNIA CIVIL CODE SECTION 1798, *et seq*.

(on behalf of Plaintiffs and the California Subclass)

163. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

164. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides: any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; (B) Injunctive or declaratory relief; (C) Any other relief the court deems proper.

165. Defendant is a "business" under § 1798.140(d) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.[45]

166. Plaintiffs and Class Members are covered "consumers" under § 1798.140(i) in that they are natural persons who are California residents.

167. The personal information of Plaintiffs and Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes but is not limited to: sensitive genetic information, names, sex, date of birth, genetic ancestry results, profile photos and geographical information.

168. Defendant knew or should have known that its data security systems and practices were inadequate to safeguard the Plaintiffs' and Class Members' Private Information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information of Plaintiffs and the Class Members. Specifically, Defendant subjected Plaintiffs' and Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of

[45] *23andMe Reports FY2023 Third Quarter Financial Results*, 23&ME, https://investors.23andme.com/news-releases/news-release-details/23andme-reports-fy2023-third-quarter-financial-results#:~:text=23andMe%20is%20raising%20its%20full,of%20%24325%20to%20%24335%20million (last accessed Oct. 25, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

169. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the loss of Plaintiffs' and the Class Members' legally protected interest in the confidentiality and privacy of their Private Information, and additional losses described above.

170. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages. *See* Section 1798.150(b). Accordingly, Plaintiffs and Class Members seek actual pecuniary damages suffered as a result of Defendant's violations described herein. Plaintiffs will issue a notice of these alleged violations pursuant to § 1798.150(b) and intends to amend this complaint to seek statutory damages upon expiration of the cure period pursuant to § 1798(a)(1)(A)(B), (a)(2), and (b).

COUNT FOUR

VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT

CALIFORNIA CIVIL CODE SECTION 1750, *et seq.*

(*on behalf of Plaintiffs and the Nationwide Class*)

171. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

172. The CLRA prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of goods.

173. Defendant's acts and practices were intended to and resulted in the sales of products and services consumers, in violation of Civil Code § 1770, including by:

a. Representing that goods or services have characteristics that they do not have, § 1770 (a)(5);

b. Representing that goods or services are of a particular standard, quality, or grade when they were not, § 1770 (a)(7);

c. Advertising goods or services with intent not to sell them as advertised, § 1770 (a)(9); and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not, § 1770 (a)(16).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

174. Defendant fraudulently deceived Plaintiffs and the Class by representing that its Products and services have certain characteristics, benefits, and qualities which they do not have, namely **data protection and security**. In doing so, Defendant intentionally misrepresented and concealed material facts from Plaintiffs and the Class, specifically by advertising secure protective measures when Defendant in fact failed to institute adequate security measures and neglected system vulnerabilities that led to the Data Breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiffs and the Class Members and depriving them of their legal rights and money. Plaintiffs and the Class Members relied on Defendant's misrepresentations regarding data protection and security in making their decisions to use Defendant's products and services, which they would not have otherwise used.

175. Defendant's claims about the products and services led and continues to lead consumers like Plaintiffs to reasonably believe that Defendant has implemented adequate data security measures when Defendant in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access consumers' Private Information.

176. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

177. Defendant knew or should have known that adequate security measures were not in place and that consumers' Private Information was vulnerable to a data breach.

178. Plaintiffs and the Class Members have suffered injury in fact as a result of and in reliance upon Defendant's false representations.

179. Plaintiffs and the Class Members would not have used the services, had they known that their Private Information would be vulnerable to a data breach. No customer would purchase Defendant's Products or use Defendant's services had they known that Defendant's data protection was inferior.

180. Defendant's actions as described herein were done with conscious disregard of Plaintiffs' rights, and Defendant was wanton and malicious in its concealment of the same.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

181. Plaintiffs and the Class Members have suffered injury in fact and have lost money as a result of Defendant's unfair, unlawful, and fraudulent conduct. Specifically, Plaintiffs paid for Products and services advertised as secure, and consequentially entrusted Defendant with their Private Information, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class Members would not have used the products and services, and would not have provided Defendant with their Private Information, had they known that their Private Information was vulnerable to a data breach.

182. Defendant should be compelled to implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiffs and the members of the Class Members lost money as a result of Defendant's unlawful practices.

183. At this time, Plaintiffs seek injunctive relief under the CLRA pursuant to Cal. Civ. Code 1782(d); but they anticipate needing to amend the complaint and seek damages and restitution.

COUNT FIVE

NEGLIGENCE

(*On behalf of Plaintiffs and Nationwide Class)*

184. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

185. Defendant owed a duty to Plaintiffs to exercise due care in collecting, storing, and safeguarding their PII. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that individuals' PII was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

186. Defendant also had a duty to destroy Plaintiffs' and Class Members' PII/PHI within an appropriate amount of time after it was no longer required by Defendant, in order to mitigate the risk of the stale PII/PHI being compromised in a data breach.

187. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

including Plaintiffs and members of the Class, who were the foreseeable and probable victims of any inadequate security practices.

188. Defendant had a special relationship with Plaintiffs and Class Members, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach. Plaintiffs and Class Members were compelled to entrust Defendant with their PII. At relevant times, Plaintiffs and Class Members understood that Defendant would take adequate security precautions to safeguard that information. Only Defendant had the ability to protect Plaintiffs' and Class Members' PII stored on Defendant's database.

189. Defendant knew of or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and Class Members, the critical importance of providing adequate security of that Private Information, the current cyber scams being perpetrated, and that they had inadequate employee training and education and IT security protocols in place to secure the Private Information of Plaintiffs and Class Members.

190. Defendant knew or should have known that Plaintiffs' and the Class Members' PII is information that is frequently sought after by hackers.

191. Defendant knew or should have known that Plaintiffs and the Class members would suffer harm if their Private Information was leaked.

192. Defendant knew or should have known that adequate and prompt notice of the data breach was required such that Plaintiffs and the Class could have taken more swift and effective action to change or otherwise protect their Private Information, rather than waiting seven (7) days to become aware of the breach and notify affected individuals, months after. Defendant failed to provide timely notice upon discovery of the data breach.

193. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and the Class Members' PII/PHI by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Defendant did not implement, design, or maintain adequate measures to detect a data breach when it occurred.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

194. Defendant and the Class entered into a special relationship when the Class Members entrusted Defendant to protect their PII. Plaintiffs and the Class trusted Defendant and in doing so provided Defendant with their PII, based upon Defendant's representations that it would implement adequate systems to secure their information. Defendant did not do so.

195. Defendant breached its duty in this relationship to implement and maintain reasonable measures to protect the Private Information of all users.

196. Plaintiffs and the Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of its duties. The leak of Plaintiffs' and the Class Members' Private Information, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

197. Defendant's negligence was, at least, a substantial factor in causing Plaintiffs and the Class's Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing the Class Members' other injuries because of the data breaches.

198. The damages suffered by Plaintiffs and the Class Members was the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiffs' and the Class Members' Private Information. Defendant knew or should have known that its security for safeguarding Plaintiffs' and the Class Members' Private Information was vulnerable to a data breach.

199. Defendant's negligence directly caused significant harm to Plaintiffs and the Class. Specifically, Plaintiffs and the Class are now subject to numerous attacks, including various phishing scams and identity theft.

200. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

201. Defendant had a fiduciary duty to protect the confidentiality of its communications with Plaintiffs and members of the Class by virtue of the explicit privacy representations Defendant made on its website to Plaintiffs and members of the Class.

202. Defendant had information relating to Plaintiffs and members of the Class that it knew or should have known to be confidential.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

203. Defendant breached its fiduciary duty of confidentiality by designing their data protection systems in a way to allow for a data breach of a massive caliber.

204. At no time did Plaintiffs or members of the Class give informed consent to Defendant's conduct.

205. As a direct and proximate cause of Defendant's actions, Plaintiffs and the Class suffered damage in that the information they intended to remain private is no longer so and their PII was intercepted by the third-parties without their knowledge or consent.

COUNT SIX

INVASION OF PRIVACY

Unauthorized Interception, Use, and Disclosure

(*On Behalf of Plaintiffs and the Nationwide Class*)

206. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

207. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their Private Information and Defendant failed to adequately protect against unauthorized access to parties.

208. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

209. Defendant failed to protect and released to unknown and unauthorized third parties the Private Information of Plaintiffs and Class Members.

210. By failing to keep Plaintiffs' and Class Members' Private Information safe, knowingly utilizing the unsecure systems and practices, Defendant unlawfully invaded Plaintiffs' and Class Member's privacy by, among others, (i) intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons; and (iii) enabling the disclosure of Plaintiffs' and Class Members' Private Information without consent.

211. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

212. Defendant knew, or acted with reckless disregard of the fact that, health care organizations were highly vulnerable to cyberattacks and thus, using inadequate security software was vulnerable to data breaches prior to the Data Beach.

213. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted and caused damages to Plaintiffs and Class Members.

214. Plaintiffs seek injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and Class Members. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT SEVEN

BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiffs and the Nationwide Class)

215. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

216. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of their use of Defendant's services. By providing their Private Information, and upon Defendant's acceptance of such information, Plaintiffs and all Class Members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts concerning genetic testing or other services to be provided by Defendant to Plaintiffs.

217. These implied-in-fact contracts obligated Defendant to take reasonable steps to secure and safeguard Plaintiffs' and other Class Members' Private Information. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards alleged above, and Defendant expressly assented to these terms in its Notice of Privacy Practices and other public statement described above.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

218. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their Private Information from unauthorized disclosure.

219. In its written privacy policies, Defendant expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.[46]

220. Defendant promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

221. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Private Information was Defendant's obligation to (a) use such Private Information for business purposes only; (b) take reasonable steps to safeguard that Private Information; (c) prevent unauthorized disclosures of the Private Information; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses; and (f) retain the Private Information only under conditions that kept such information secure and confidential.

222. Without such implied contracts, Plaintiffs and Class Members would not have provided their Private Information to Defendant.

223. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to conduct the following: 1) reasonably safeguard and protect Plaintiffs' and Class Members' Private Information, which was compromised as a result of the Data Breach; 2) comply with its promise to abide by HIPAA; 3) ensure the confidentiality and integrity of electronic protected health information that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R 164.306(a)(1); 4) implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in

[46] *See supra*, ¶¶ 69-78.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

violation of 45 C.F.R 164.312(a)(1); 5) implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R 164.308(a)(1); 6) identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R 164.308(a)(6)(ii); and 7) protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2).

224. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and other Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, and Plaintiffs and other Class Members have been put at an increased risk of identity theft, fraud, and/or misuse of their Private Information, which may take months if not years to manifest, discover, and detect.

COUNT EIGHT

CONVERSION

(*On behalf of Plaintiffs and the Nationwide Class*)

225. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

226. Plaintiffs and Class Members were the owners and possessors of their Private Information.

227. Courts recognize that internet users have a property interest in their personal information and data. *See Calhoun v. Google, LLC,* 526 F. Supp. 3d 605, at *21 (N.D. Cal. Mar. 17, 2021) (recognizing property interest in personal information and rejecting Google's argument that "the personal information that Google allegedly stole in not property"); *In re Experian Data Breach Litigation,* 2016 U.S. Dist. LEXIS 184500, at *5 (C.D. Cal. Dec. 29, 2016) (loss of value of PII is a viable damages theory); *In re Marriott Int'l Inc. Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 460 (D. Md. 2020) ("The growing trend across courts that have considered this issue is to

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

recognize the lost property value of this [personal] information."); *Simona Opris v. Sincera,* 2022 U.S. Dist. LEXIS 94192, (E.D Pa. 2022) (collecting cases).

228. The economic value of this property interest in personal information is well understood, as a robust market for such data drives the entire technology economy. As experts have noted, the world's most valuable resource is "no longer oil, but data," and has been for years now.[47]

229. As the result of Defendant's wrongful conduct, Defendant has interfered with Plaintiffs' and Class Members' rights to possess and control such property, to which they had a superior right of possession and control at the time of conversion.

230. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class Members suffered injury, damage, loss or harm.

231. In failing to adequately safeguard Plaintiffs' Private Information, Defendant has acted with malice, oppression and in conscious disregard of the Plaintiffs' and Class Members' rights.

232. Plaintiffs and the Class Members did not consent to Defendant's mishandling and loss of their Private Information.

233. Plaintiffs seek injunctive relief restitution and all other damages available under this cause of action.

COUNT NINE

BREACH OF CONFIDENCE

(*On behalf of Plaintiffs and the Nationwide Class*)

234. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

235. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information that Plaintiffs and Class Members provided to Defendant.

[47] *The world's most valuable resource is not longer oil, but data.* THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but data?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=17210591673&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=1&gclid=EAIaIQobChMIrsDb8bqUggMVCLCGCh3h_A9zEAAYASAAEgKOsPD_BwE&gclsrc=aw.ds (last accessed Oct. 26, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

236. Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

237. Plaintiffs and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit their Private Information to be disseminated to or accessed by any unauthorized third parties.

238. Plaintiffs and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

239. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Private Information with the understanding that Private Information would not be disclosed to or accessed by unauthorized third parties.

240. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

241. As a proximate result of such unauthorized disclosures, Plaintiffs and Class Members suffered damages.

242. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, access, and used by unauthorized third parties.

243. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's inadequate security of Plaintiffs' and Class Members' Private Information.

244. Defendant knew or should have known that its methods of accepting, storing, transmitting, and using Plaintiffs' and Class Members' Private Information was inadequate.

245. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury, including but not limited to: (i) threat of identity theft; (ii) the loss

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, medical fraud, and/or unauthorized use of their Private Information; (v) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

246. As a direct proximate result of such unauthorized disclosures, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT TEN

UNJUST ENRICHMENT

(On behalf of Plaintiffs and the Nationwide Class)

247. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

248. Plaintiffs and Class Members conferred a monetary benefit on Defendant—namely, they provided and entrusted Defendant with their Private Information. Upon information and belief, Defendant funds its data security measures entirely from payments made by or on behalf of Plaintiffs and the Class Members. Accordingly, a portion of such payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

249. In exchange for this payment, Plaintiffs and Class Members should have been entitled to have Defendant protect their Private Information with adequate data security.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

250. Defendant appreciated, accepted, and retained the benefit bestowed upon them under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and Class Members as described herein – namely, (a) Plaintiffs and Class Members conferred a benefit on Defendant, and Defendant accepted or retained that benefit; and (b) Defendant used Plaintiffs' and Class Members' Private Information for business purposes.

251. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

252. Defendant acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

253. Plaintiffs and Class Members have no adequate remedy at law.

254. Under the circumstances, it would be unjust and unfair for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred on it.

255. Under the principles of equity and good conscience, Defendant should not be permitted to retain the Private Information belonging to Plaintiffs and Class Members because Defendant failed to implement the data management and security measures that industry standards mandate.

256. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from the use of Plaintiffs' and Class Members' Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for judgment and relief on all cause of action as follows:

A. That this Action may be maintained as a Class Action, that Plaintiffs be named as Class Representatives of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. An order:

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's failure to provide adequate notice to all affected individuals);

b. Requiring Defendant to implement adequate security protocols and practices to protect individuals' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected individuals, and posted publicly;

d. Requiring Defendant to protect all data collected through its account creation requirements;

e. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

is compromised, hackers cannot gain access to other portions of Defendant's systems

j. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

k. Requiring Defendant to conduct systematic scanning for data breach related issues;

l. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the PII/PHI data;

m. Requiring Defendant to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

n. Requiring Defendant to implement a system of testing to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting Private Information;

o. Requiring Defendant to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor Defendant information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; and

p. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

C. That the Court award Plaintiffs and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiffs and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

E. Plaintiffs and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

F. Plaintiffs and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

G. Plaintiffs and the Class be awarded with treble and/or punitive damages insofar as they are allowed by applicable laws; and

H. Any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Plaintiffs demand a jury trial on all triable issues.

DATED: October 26, 2023

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart
Ryan Clarkson, Esq.
Yana Hart, Esq.
Tiara Avaness, Esq.
Valter Malkhasyan, Esq.

Counsel for Plaintiffs and the Proposed Classes

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com